PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 05 April 2000 (05.04.00)	
International application No. PCT/GB99/02672	**Applicant's or agent's file reference** PLB/CC/Q419
International filing date (day/month/year) 12 August 1999 (12.08.99)	**Priority date** (day/month/year) 20 August 1998 (20.08.98)
Applicant ABDULHAYOGLU, Melih	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

19 February 2000 (19.02.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Juan Cruz
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00

A1

(11) International Publication Number: WO 00/11537

(43) International Publication Date: 2 March 2000 (02.03.00)

(21) International Application Number: PCT/GB99/02672

(22) International Filing Date: 12 August 1999 (12.08.99)

(30) Priority Data:
9818186.0 20 August 1998 (20.08.98) GB

(71) Applicant *(for all designated States except US)*: COMODO TECHNOLOGY DEVELOPMENT LIMITED [GB/GB]; 10 Hey Street, Bradford, West Yorkshire BD7 1DQ (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: ABDULHAYOGLU, Melih [TR/GB]; 10 Hey Street, Bradford, West Yorkshire BD7 1DQ (GB).

(74) Agents: BRANDON, Paul, Laurence et al.; Appleyard Lees, 15 Clare Road, Halifax, West Yorkshire HX1 2HY (GB).

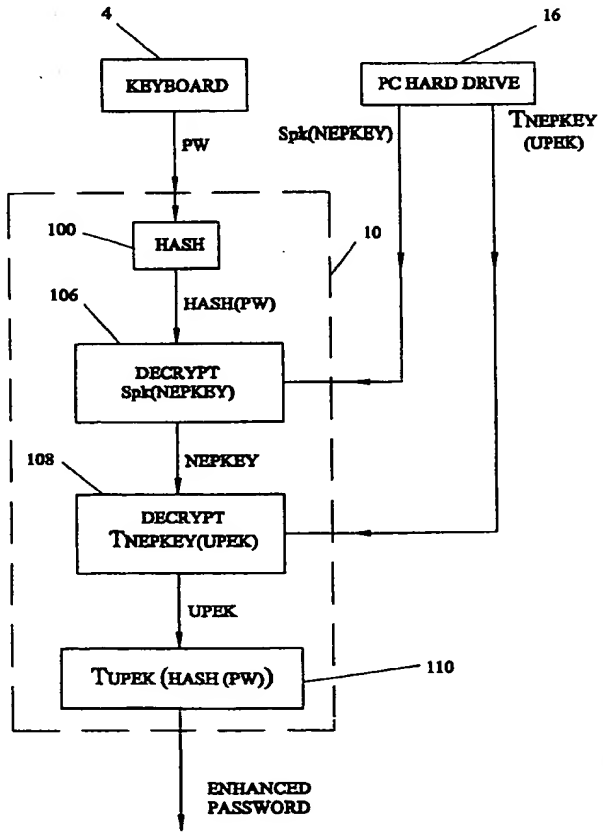
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: IMPROVEMENTS IN AND RELATING TO DATA COMMUNICATION

(57) Abstract

The present invention provides a method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password. Preferred embodiments of the present invention provide for more secure password handling, by enhancing the password.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

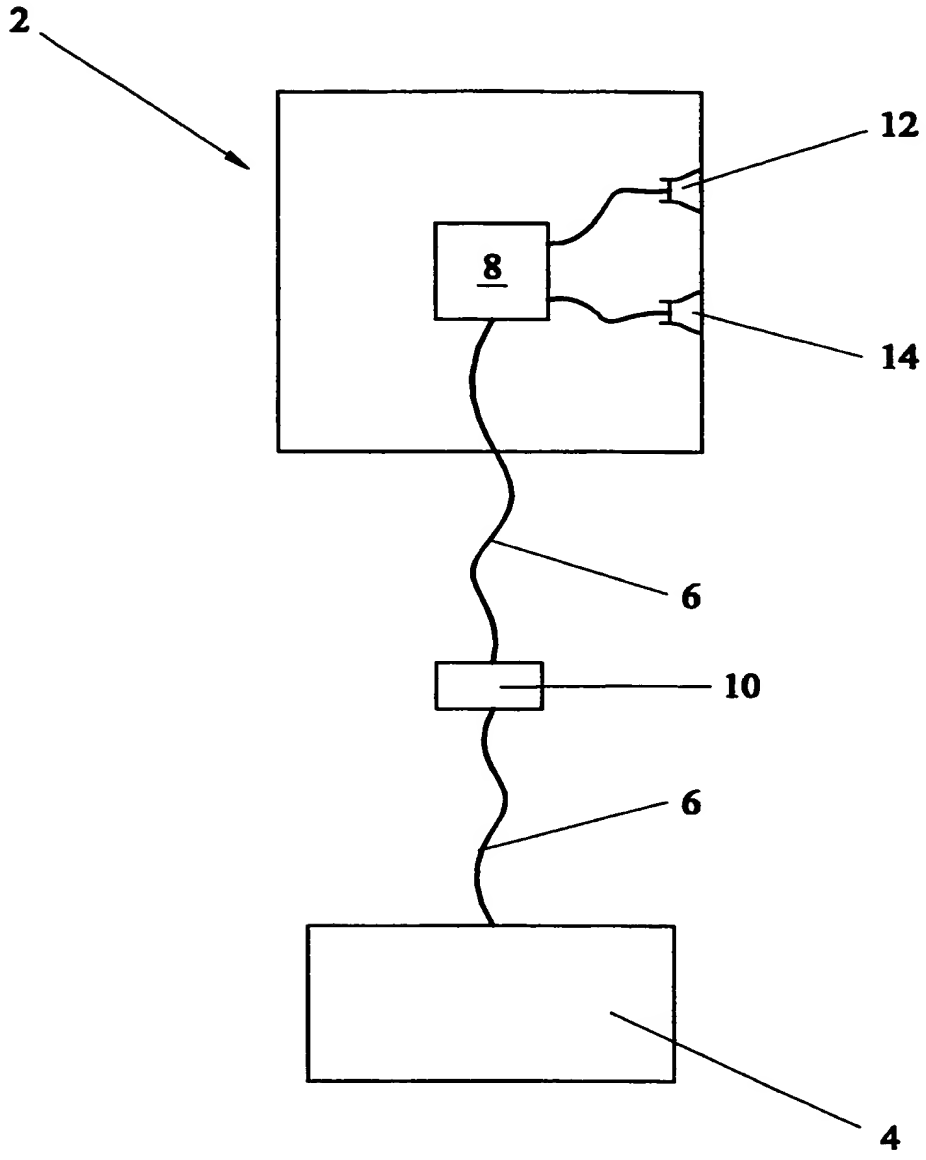


FIG. 1

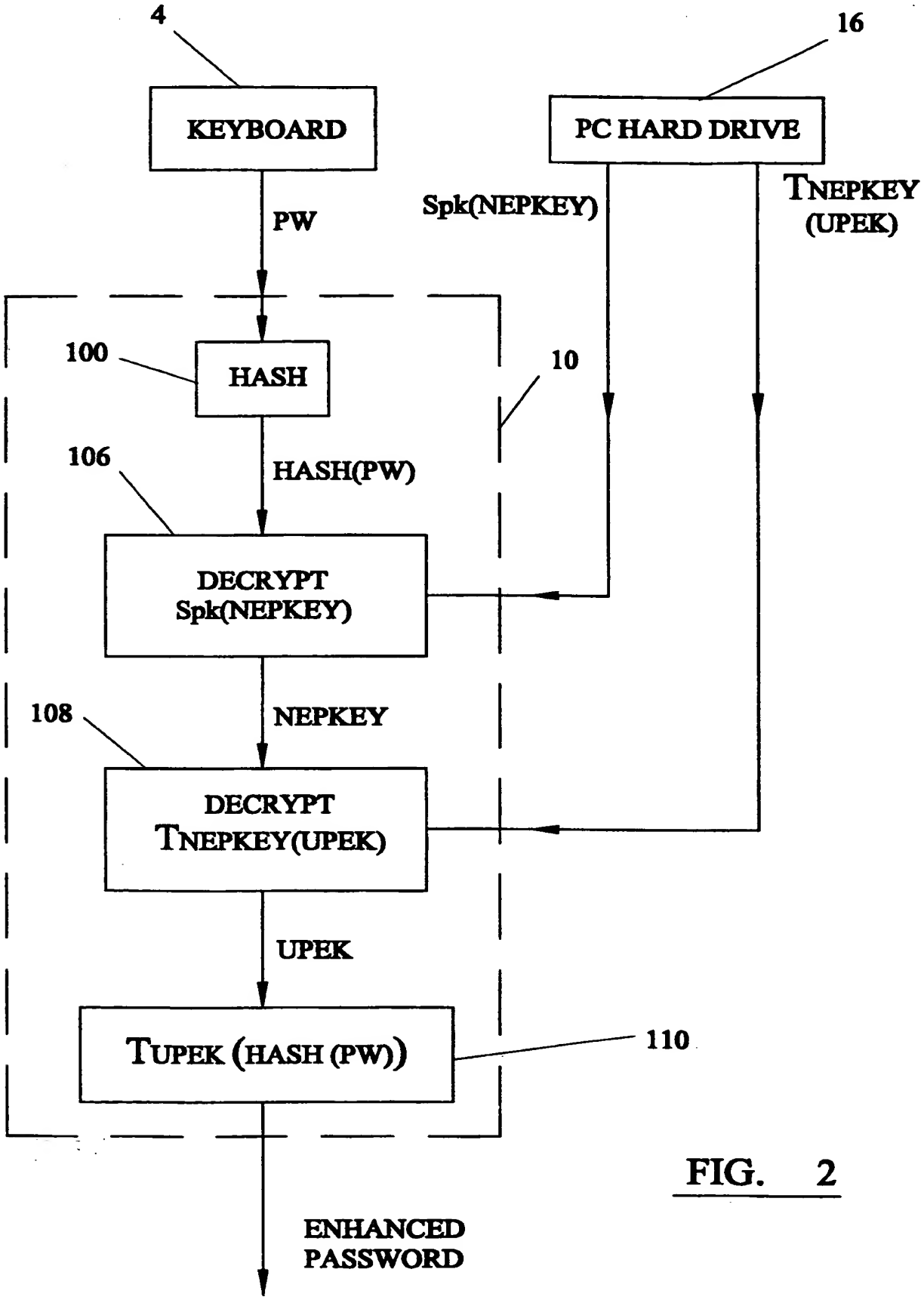

4
KEYBOARD
16
PC HARD DRIVE
PW
Spk(NEPKEY)
TNEPKEY
(UPEK)
100
HASH
10
106
HASH(PW)
DECRYPT
Spk(NEPKEY)
108
NEPKEY
DECRYPT
TNEPKEY(UPEK)
UPEK
TUPEK (HASH (PW))
110
ENHANCED
PASSWORD

FIG. 2

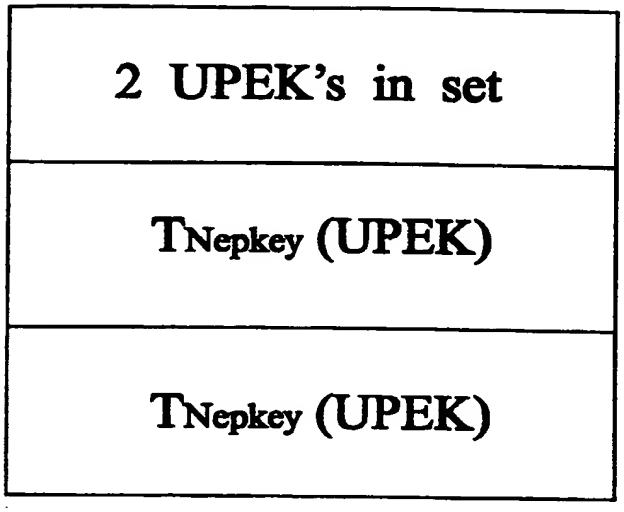


FIG. 3

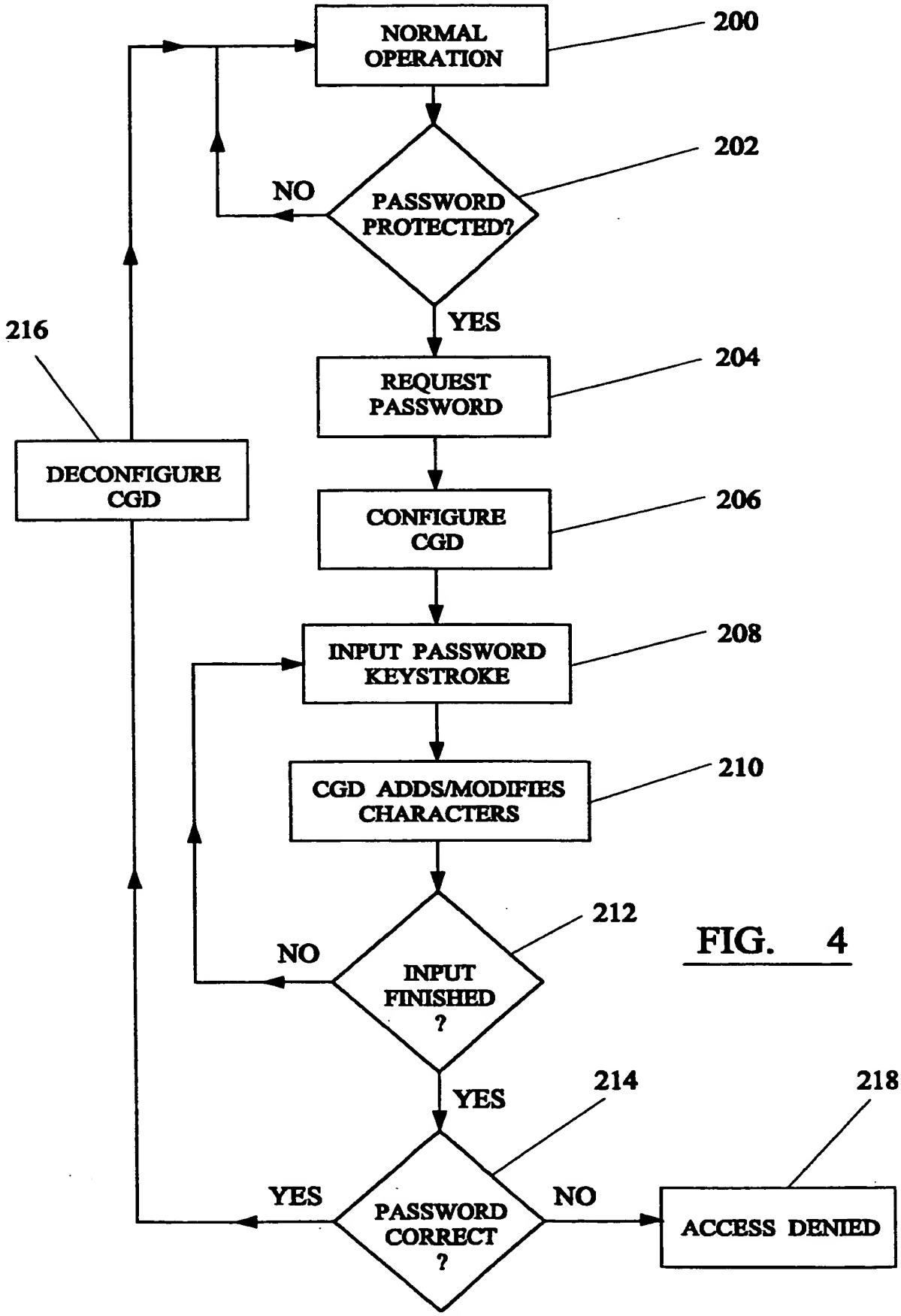

NORMAL OPERATION
200
PASSWORD PROTECTED?
202
NO
YES
REQUEST PASSWORD
204
CONFIGURE CGD
206
INPUT PASSWORD KEYSTROKE
208
CGD ADDS/MODIFIES CHARACTERS
210
INPUT FINISHED ?
212
NO
YES
PASSWORD CORRECT ?
214
YES
NO
ACCESS DENIED
218
DECONFIGURE CGD
216

FIG. 4

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/GB 99/02672

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 768 373 A (GRAWROCK DAVID ET AL) 16 June 1998 (1998-06-16) the whole document	1-5,7-10
A		6,14,15, 22

X	EP 0 809 171 A (SCHLUMBERGER TECHNOLOGIES INC) 26 November 1997 (1997-11-26) abstract; figure 1 column 6, line 40 - line 55	11, 14-17, 22-24
Y		12,13, 18-21,25

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 December 1999	10/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/GB 99/02672

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 677 952 A (ROGAWAY PHILLIP W ET AL) 14 October 1997 (1997-10-14) abstract; figure 3 claim 20	12,13,25
A		9,10
Y	EP 0 549 511 A (IBM) 30 June 1993 (1993-06-30) abstract; figures 1,4 column 1, line 1 -column 2, last line column 4, line 22 - line 29 claims 1-8	18-21
A	WO 95 26085 A (CLARK DERECK B ;INNOVONICS INC (US)) 28 September 1995 (1995-09-28)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter[illegible]onal Application No
PCT/GB 99/02672

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5768373 A	16-06-1998	EP 0894377 A	03-02-1999
		WO 9742732 A	13-11-1997
EP 0809171 A	26-11-1997	US 5832206 A	03-11-1998
		CA 2197027 A	26-09-1997
US 5677952 A	14-10-1997	US 5454039 A	26-09-1995
		EP 0658022 A	14-06-1995
		JP 7199808 A	04-08-1995
		SG 44363 A	19-12-1997
		US 5675652 A	07-10-1997
		US 5835597 A	10-11-1998
EP 0549511 A	30-06-1993	US 5664097 A	02-09-1997
		JP 5233087 A	10-09-1993
WO 9526085 A	28-09-1995	US 5517569 A	14-05-1996
		AU 691602 B	21-05-1998
		AU 2190295 A	09-10-1995
		BR 9507114 A	02-09-1997
		CA 2185697 A	28-09-1995
		EP 0750812 A	02-01-1997
		JP 10500504 T	13-01-1998
		NZ 283566 A	19-12-1997
		US 5815577 A	29-09-1998

IMPROVEMENTS IN AND RELATING TO DATA COMMUNICATION

Field of the Invention

The present invention relates to data communication devices and methods, and to programs for executing such methods and carriers therefor.

Background to the Invention

With the growth of computer networks, including the internet, local area networks, wide area networks and intranets, additional problems have been created in relation to computer security. In particular, the possibilities for unauthorised remote access into a computer (sometimes referred to as "hacking") have been increased.

Hackers seeking unauthorised access have developed various forms of software to assist in these attacks, including those that make multiple attempts to gain access through password controlled systems. Typically such software will try various permutations of possible passwords until the correct one is found. This can either be a "dictionary" attack, restricted to known words, or a "brute force" attack which tries all permutations. For this reason, amongst others, many systems require passwords of a minimum length, but as these have to be memorised by a user only a certain minimum length is practicable. Thus, many password lengths fall in the range of 4-8 characters and are often everyday words for case of recollection. This makes a software-assisted attack on the system a real risk to any password protected function or data.

It is an aim of preferred embodiments of the present invention to obviate or overcome at least one disadvantage encountered in relation to the prior art, whether referred to herein or otherwise.

Summary of the Invention

According to the present invention in a first aspect, there is provided a method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password.

Preferred embodiments of the present invention provide for more secure password handling, by enhancing the password.

Suitably, the encryption comprises a hash operation.

Suitably, the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH). Suitably, the first stored key is encrypted by a public key encryption algorithm.

Suitably, the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY). Suitably, the second stored key is encrypted by a reversible algorithm.

Suitably, the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

According to the present invention in a second aspect, there is provided a data access method comprising the steps of producing an enhanced password according to the first aspect of the present invention, comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond.

The data to be accessed may be any type, including a file, an application, a data record etc.

According to the present invention in a third aspect there is provided a computer program for carrying out the method of the second aspect of the present invention.

According to the present invention in a fourth aspect, there is provided a carrier comprising a program according to the third aspect of the invention.

According to the present invention in a fifth aspect, there is provided a data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator.

Suitably, the output signal is of a different length to the signal input to the character generator. More suitably, the output signal is longer than the signal input to the character generator.

Suitably, the system further comprises means for comparing the output signal with a stored password. More suitably, the comparison means further comprises means for outputting a signal dependent upon the correspondence of the output signal with the stored password.

Suitably, the input device comprises a keyboard.

Suitably, the set of available input signals comprises all or part of the character set of the keyboard.

Suitably, the system comprises a first input and a second input in which the character generator receives signals from the first input and does not receive signals from the second input.

Suitably, the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection.

Suitably, the input signal comprises or corresponds to one of the set of input signals.

Suitably, the set of input signals comprises alphanumeric characters.

According to the present invention in a sixth aspect, there is provided a digital computer comprising a data communication system according to the fifth aspect of the invention.

According to the present invention in a seventh aspect, there is provided a data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal.

Suitably, the method further comprises the step of repeating the operation for a plurality of input signals.

Suitably, the output signals vary in length one from the other.

Suitably, the method according to the eighth aspect of the invention is modified according to the sixth aspect of the invention.

Brief Description of the Drawings

The present invention will now be described, by way of example only, with reference to the drawings that follow; in which:

Figure 1 is a schematic functional illustration of an embodiment of the present invention.

Figure 2 is a functional flow diagram illustrating operation of a preferred embodiment of the present invention.

Figure 3 is a diagram showing how data is stored according to the embodiment of the present invention described in relation to Figure 2.

Figure 4 is a functional flow diagram of the operation of the character generating device of the present invention in another embodiment.

Description of the Preferred Embodiments

Referring to Figure 1 of the drawings that follow, there is shown an electronic digital computer 2, typically a personal computer ("PC") comprising a keyboard 4 connected via a data line 6 to a processor 8. Those skilled in the art will appreciate that various elements intervene between the keyboard and processor.

On the data line 6 between keyboard 4 and processor 8 is a character generating device 10. The initials "CGD" are used for character generating device in this specification.

Other input ports 12, 14 as also shown which may for instance, be from a modem.

The character generating device 10 is configured to controllably modify the output of keystrokes from keyboard 4 to produce additional output for password verification, until that password verification is achieved and then revert to normal keyboard output operation.

The operation of the device will now be described in more detail with reference to Figures 2 onwards of the drawings that follow.

Upon activation of the application a password is requested to be input and the number of characters of an

enhanced password is set. The input is "filtered" to recognise non-character codes such as CTRL and <SHIFT> so that these are not required in the user's password.

Referring now to Figure 2 of the drawings that follow, the keyboard 4, CGD 10 and a PC hard drive 16 are outlined. A user password (PW) is entered from keyboard 4. For purposes of explanation let the user password input be "BOB". The user sets the enhanced password length to, say, 10 characters. Upon an <ENTER> key strike (or typically for a WINDOWS (Registered Trade Mark) application, clicking the "OK" button) the user password BOB is enhanced.

Each CGD 10 contains a common key referred to as a NEPKEY. The CGD 10 uses a secret public key encryption algorithm with its own unique public key (the public key differs between CGD devices) to encrypt the NEPKEY, the result of which, referred to as Spk(NEPKEY) is stored on the PC hard drive. Thus the NEPKEY itself is not known outside of the CGD 10.

The CGD 10 creates a User Password Enchancer Encryption Key, referred to as UPEK, in a function called "GUPEK". A UPEK is generated in the CGD 10 as a random number. It need not be a random number, the main requirement being it is not known outside of the CGD 10. Each CGD 10 has the same NEPKEY (or set of NEPKEYs as several may be used), but a unique UPEK (or set thereof).

GUPEK is passed the Spk(NEPKEY) to be used to encrypt a new UPEK, how many new UPEK's are to within the set, and the location of the temporary resident program that can create UPEKs. It then passed the CGD 10 the encrypted

NEPKEY (ie $T_{NEPKEY}(UPEK)$, where T is a symmetric encryption algorithm). As each new UPEK is created, according to the number to be generated, the CGD 10 encrypts it with the NEPKEY (ie $T_{NEPKEY}(UPEK)$). When it has finished, the temporary resident program is unloaded from the CGD 10. The CGD 10 then adds the encrypted UPEKs to one block of data, with a header 102 containing how many UPEKs 104a, 104b are within the set, as shown in Figure 3 of the drawings that follow. The NEPKEY encrypted UPEK is saved on the hard drive. Thus the UPEK is not known outside of the CGD 10. The generation of the Spk(NEPKEY) and T_{NEPKEY} (UPEK) are carried out in the set-up stage. There may be several UPEKs in a CGD 10.

At 100 the input user password is hashed to generate an output of predictable length, in this case 16 bytes. The primary reason for the HASH operation is to produce an irreversible result.

In the enhanced password generation method, at 106 the encrypted NEPKEY is retrieved from the PC hard drive 16 and decrypted by the CGD 10 to obtain the NEPKEY. Next at 108 the NEPKEY encrypted UPEK is retrieved and decrypted by the CGD 10 using the NEPKEY decrypted at 106 to obtain the UPEK.

The UPEK is encrypted by the HASH output from 100 and an enhanced password output of desired character length output. This enhanced password is stored, usually in the header portion of an application or document.

When access is sought to the application or document, the password enhancing application is activated and upon a

user password being entered it is password enhanced as set out above, the result being compared with the password stored for the application or document. This comparison is carried out by the application itself, not by the CGD 10 that produces the enhanced password. As a modification the password checking can be carried out by the CGD 10 if it is loaded with appropriate software.

The CGD 10 is configured so that it will only accept one user password per second. The gap between acceptable inputs for password enhancing can be varied to provide additional security.

New NEPKEYs can be entered when required, preferably from a secure source so that the NEPKEY cannot be intercepted.

The HASH operation output length can be varied as a matter of design device. Normally it will be 64 to 128 bytes.

This system has several advantages as set out below:

(i) the user password is not stored on the PC so it cannot be retrieved by a hacker;

(ii) the relationship between the keyboard input and the CGD output (ie the enhanced password) is such that there is no practical reversibility;

(iii) by only permitting one password entry every second or so the system substantially prevents brute force attacks on the password. To succeed in a brute

force attack a large number of permutations must be tried. At one entry per second the time required for a dictionary or brute force attack is unfeasible. For instance, at one million entries per second an six character password, with each character being selected from a possible 72 character set has 139,314,069,504 possible combinations that would take nearly 38 hours to try by brute force. If entry were restricted to one entry per second, the brute force attack would take 4417 years; and

(iv) because of the shared NEPKEY, hot seating (i.e. the use of different machines by one user) can be accommodated even though the CGD 10 on each machine has a different public key. The UPEK('s) associated with the particular user can be transferred securely between machines by encoding using the NEPKEY as a key ie T_{NEPKEY} (UPEK). It is noted that neither the NEPKEY(s) nor the UPEK(s) are seen or inspectable in plain (ie unencrypted) text outside of the secure CGD 10.

If desired new NEPKEYs can be downloaded into the CGD 10 using a security protocol.

A further embodiment of the present invention will now be described with reference to Figure 4 of the drawings that follow.

From a mode 200 in which the PC 2 is operating normally, an access is requested either to functions or data, the PC checks 202 to determine whether the function

or data (say a file) is password protected. If not, the "NO" branch is followed and normal operation resumes with access permitted. If the function or data is password protected, the "YES" branch is followed and a suitable password is requested 204 and the character generating device is configured 206 to output additional characters according to a predetermined scheme.

Then, as each keystroke of the password is input 208 the signal is received by the device 10 and a corresponding longer output is generated 210. Thus, by way of example, if the keystroke "F" is entered, the device may output "P7TTWR0". The actual output is substantially immaterial so long as it is in accordance with a predetermined relationship between the input key and output sequence from the device 10.

The system then determines if the password input is finished 212. This may be by detecting the input of a <ENTER> key, the length of input or some other characteristic . If the input is not finished, the system requires a further input keystroke. If the input is finished, the "YES" branch is followed and the input password is compared with a password in memory 214. If the password is correct, the "YES" branch is followed, the character generator is configured 216 so input passes normally access to the function or data is permitted and normal operation resumed. If the password is incorrect, the "NO" branch is followed and access is denied 218.

Instead of access being denied on the first entry of an incorrect password, several attempts can be permitted, but normally not an unlimited number.

In addition to access being defined upon entry of incorrect password, additional alarm functions may be actuated.

The original password may also be input using this method and device. The user need never know or be concerned with the longer version of their password.

Accordingly, using the present invention it is possible for a user to remember a relatively short password, say "FRED" but for the processor to require validation of a much longer password which may or may not include the original password elements. By way of example, keyboard keystrokes of "FRED" at the password request stage may generate: P7aTWR0X3NR?B2aR88CI9CcAB.

So, a password input keystroke of four characters generates a twenty-six character long password for verification.

The device and system is configured so that remote access to the PC 2 is not via the device 10 so that such remote access requires entry of the full (longer) password required by the processor. Accordingly, protection from external hacking is enhanced.

The present invention can be embodied in hardware and/or software. Typically, in a hardware embodiment the device is located in a keyboard.

The "passwords" referred to herein may be of any signal or combination of signals and need not be "words" at all.

While the present embodiment has been described for use on a PC, it will be appreciated that the present invention can equally be put into effect on other platforms, devices or equipment.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any

novel combination, of the steps of any method or process so disclosed.

Claims

1. A method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password.

2. A method according to claim 1, in which the encryption comprises a hash operation.

3. A method according to claim 1 or claim 2, in which the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH).

4. A method according to claim 3, in which the first stored key is encrypted by a public key encryption algorithm.

5. A method according to claim 3 or claim 4, in which the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY).

6. A method according to claim 5, in which the second stored key is encrypted by a reversible algorithm.

7. A method according to claim 5 or claim 6, in which the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

8. A data access method comprising the steps of producing an enhanced password according to any one of claims 1 to 7,

comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond.

9. A computer program for carrying out the method of claim 8.

10. A carrier comprising a program according to claim 9.

11. A data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator.

12. A data communication system according to claim 11, in which the output signal is of a different length to the signal input to the character generator.

13. A data communication system according to claim 12, in which the output signal is longer than the signal input to the character generator.

14. A data communication system according to any one of claims 11 to 13, in which the system further comprises means for comparing the output signal with a stored password.

15. A data communication system according to claim 14, in which the comparison means further comprises means for

outputting a signal dependent upon the correspondence of the output signal with the stored password.

16. A data communication system according to any one of claims 11 to 15, in which the input device comprises a keyboard.

17. A data communication system according to claim 16, in which the set of available input signals comprises all or part of the character set of the keyboard.

18. A data communication system according to any one of claims 11 to 17, in which the system comprises a first input and a second input in which the character generator receives signals from the first input and does not receive signals from the second input.

19. A data communication system according to claim 18, in which the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection.

20. A data communication system according to claim 19, in which the input signal comprises or corresponds to one of the set of input signals.

21. A data communication system according to claim 20, in which the set of input signals comprises alphanumeric characters.

22. A digital computer comprising a data communication system according to any one of claims 11 to 21.

23. A data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal.

24. A method according to claim 23, in which the method further comprises the step of repeating the operation for a plurality of input signals.

25. A method according to claim 23 or claim 24, in which the output signals vary in length one from the other.

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/GB 99/02672

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 768 373 A (GRAWROCK DAVID ET AL) 16 June 1998 (1998-06-16) the whole document	1-5,7-10
A		6,14,15, 22

X	EP 0 809 171 A (SCHLUMBERGER TECHNOLOGIES INC) 26 November 1997 (1997-11-26) abstract; figure 1 column 6, line 40 - line 55	11, 14-17, 22-24
Y		12,13, 18-21,25

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 December 1999	10/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/GB 99/02672

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 677 952 A (ROGAWAY PHILLIP W ET AL) 14 October 1997 (1997-10-14) abstract; figure 3 claim 20	12,13,25
A	---	9,10
Y	EP 0 549 511 A (IBM) 30 June 1993 (1993-06-30) abstract; figures 1,4 column 1, line 1 -column 2, last line column 4, line 22 - line 29 claims 1-8	18-21
A	--- WO 95 26085 A (CLARK DERECK B ;INNOVONICS INC (US)) 28 September 1995 (1995-09-28) -----	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/GB 99/02672

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5768373 A	16-06-1998	EP 0894377 A	03-02-1999
		WO 9742732 A	13-11-1997
EP 0809171 A	26-11-1997	US 5832206 A	03-11-1998
		CA 2197027 A	26-09-1997
US 5677952 A	14-10-1997	US 5454039 A	26-09-1995
		EP 0658022 A	14-06-1995
		JP 7199808 A	04-08-1995
		SG 44363 A	19-12-1997
		US 5675652 A	07-10-1997
		US 5835597 A	10-11-1998
EP 0549511 A	30-06-1993	US 5664097 A	02-09-1997
		JP 5233087 A	10-09-1993
WO 9526085 A	28-09-1995	US 5517569 A	14-05-1996
		AU 691602 B	21-05-1998
		AU 2190295 A	09-10-1995
		BR 9507114 A	02-09-1997
		CA 2185697 A	28-09-1995
		EP 0750812 A	02-01-1997
		JP 10500504 T	13-01-1998
		NZ 283566 A	19-12-1997
		US 5815577 A	29-09-1998

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
PLB/JE/Q419		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB99/02672	12/08/1999	20/08/1998
International Patent Classification (IPC) or national classification and IPC G06F1/00		
Applicant COMODO TECHNOLOGY DEVELOPMENT LIMITED et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☐ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
19/02/2000	13.10.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Dixon-Hundertpfund K Telephone No. +49 89 2399 2857

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB99/02672

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-14 as originally filed

Claims, No.:

1-25 as originally filed

Drawings, sheets:

1/4-4/4 as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 1-25.

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1.1 The various definitions of the invention given in independent Claims 1, 8, 9, 10, 11, 22 and 23 are such that the claims as a whole are not clear and concise, contrary to Article 6 PCT. The claims should be re-cast to include only the minimum necessary number of independent claims in any one category, with dependent claims as appropriate (Rule 6.4(a)-(c) PCT).

In the present case it is considered appropriate to use one independent claim in any category, the independent claims defining the same essential technical features and defining corresponding features in corresponding terms.

1.2 It is furthermore not clear what the essential technical features of the invention are, because the independent claims do not define corresponding features in corresponding terms and do not define the same features. For example reference is made to "entering a user password" in claims 1, 8, 9 and 10, but not in claims 11, 22 and 23, and claims 11, 22 and 23 define input and output signals , but claims 1, 8, 9 and 10 do not.

1.3 Therefore, because of the above unclarities, it is not possible to identify "the claimed invention" on which an opinion should be based in the sense of Article 33.1 PCT.

2. A full substantive examination will take place once the claims have been clarified. However the following observations are made:

i) Reference is made to the following documents:
D1: US 5 768 373 A (GRAWROCK DAVID ET AL) 16 June 1998 (1998-06-16)
D2: EP 0 809 171 A (SCHLUMBERGER TECHNOLOGIES INC) 26 November 1997 (1997-11-26)
D3: US 5 677 952 A (ROGAWAY PHILLIP W ET AL) 14 October 1997 (1997-10-14)
D4: EP 0 549 511 A (IBM) 30 June 1993 (1993-06-30)
D5: WO 95 26085 A (CLARK DERECK B ;INNOVONICS INC (US)) 28 September

1995 (1995-09-28)

In the search report, document D1 is cited as X for some of the claims, document D2 is cited as X and Y for some of the claims, and document D3 and D4 are cited as Y for some of the claims. Documents D1 to D4, either singly or in combination, are therefore of great relevance to the claims.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
PLB/CC/Q419		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/GB 99/02672	12/08/1999	20/08/1998
Applicant		
COMODO TECHNOLOGY DEVELOPMENT LIMITED et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

[ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

[ ] contained in the international application in written form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readble form.

[ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

[X] the text is approved as submitted by the applicant.

[ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

[X] the text is approved as submitted by the applicant.

[ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2

[X] as suggested by the applicant.

[ ] None of the figures.

[ ] because the applicant failed to suggest a figure.

[ ] because this figure better characterizes the invention.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 99/02672

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 768 373 A (GRAWROCK DAVID ET AL) 16 June 1998 (1998-06-16) the whole document	1-5,7-10
A		6,14,15, 22

X	EP 0 809 171 A (SCHLUMBERGER TECHNOLOGIES INC) 26 November 1997 (1997-11-26) abstract; figure 1 column 6, line 40 - line 55	11, 14-17, 22-24
Y		12,13, 18-21,25

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 December 1999	10/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 99/02672

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 677 952 A (ROGAWAY PHILLIP W ET AL) 14 October 1997 (1997-10-14) abstract; figure 3 claim 20	12,13,25
A	---	9,10
Y	EP 0 549 511 A (IBM) 30 June 1993 (1993-06-30) abstract; figures 1,4 column 1, line 1 -column 2, last line column 4, line 22 - line 29 claims 1-8	18-21
A	--- WO 95 26085 A (CLARK DERECK B ;INNOVONICS INC (US)) 28 September 1995 (1995-09-28) -----	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 99/02672

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5768373	A	16-06-1998	EP	0894377 A	03-02-1999
			WO	9742732 A	13-11-1997
EP 0809171	A	26-11-1997	US	5832206 A	03-11-1998
			CA	2197027 A	26-09-1997
US 5677952	A	14-10-1997	US	5454039 A	26-09-1995
			EP	0658022 A	14-06-1995
			JP	7199808 A	04-08-1995
			SG	44363 A	19-12-1997
			US	5675652 A	07-10-1997
			US	5835597 A	10-11-1998
EP 0549511	A	30-06-1993	US	5664097 A	02-09-1997
			JP	5233087 A	10-09-1993
WO 9526085	A	28-09-1995	US	5517569 A	14-05-1996
			AU	691602 B	21-05-1998
			AU	2190295 A	09-10-1995
			BR	9507114 A	02-09-1997
			CA	2185697 A	28-09-1995
			EP	0750812 A	02-01-1997
			JP	10500504 T	13-01-1998
			NZ	283566 A	19-12-1997
			US	5815577 A	29-09-1998